t +27 (0) 10 140 5000 e sales@saicom.io w saicom.io

PRODUCT ANNEXURE - FORTINET FIREWALL SERVICES

1. INTRODUCTION

This Annexure sets out the legal framework for the provision and use of Fortinet Firewall Services provided by the Supplier. This Product Annexure is subject to and must be read in conjunction with the Supplier terms and conditions located at https://saicom.io/ and the licensor specific documentation referred to in and located at https://www.fortinet.com/corporate/about-us/legal. The nomenclature used in the Agreement shall apply to this Product Annexure.

2. DEFINITIONS

2.1. **Application Control** - protects servers by allowing or denying network application usage based on policies established by the network administrator. Enterprise applications, databases, web mail, social networking applications, IM/P2P, and file transfer protocols can all be identified accurately by sophisticated detection signatures. Application Control signature updates are provided via the global distribution network.

2.2. **IPS** - Intrusion Prevention System detects threats against the network and/or hosted environment to proactively block attacks. The IPS Service is an integrated hardware and software platform based on best of breed architecture. IPS delivers protection from known, zero day and denial of service (DoS) attacks including malware and underlying vulnerabilities.

2.3. **Layer 2** - The data link layer, or layer 2, is the second layer of the seven-layer OSI model of computer networking. This layer is the protocol layer that transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment.

2.4. **UTP** - Unified Threat Protection consolidates multiple security and networking functions with one unified appliance that protects businesses and simplifies infrastructure.

2.5. **VDOM** - Virtual Domains are a method of dividing a FortiGate unit into two or more virtual units that function as multiple independent units.

2.6. **VPN** - Virtual Private Network. A configuration that allows remote users to connect to the Firewall, and access resources behind it securely.

2.7. N-2 - The version of Firmware applied will be 2 minor releases behind the current licensor approved release. This is dependent on new bugs/features introduced in newer versions.

2.8. **DMZ** - Demilitarized Zone - Is a network architecture concept whereby a separate zone is introduced that separates and isolates the LAN from untrusted networks(the internet). This zone usually sits between the LAN and the WAN acting as a buffer zone to protect the internal network from external threats.

2.9. **EMS** - Endpoint Management System - It is a software solution provided by Fortinet, a cybersecurity company, that is designed for managing and securing endpoints within a network, such as computers, mobile devices, and servers. EMS helps organisations centrally manage and protect their networked devices.

2.10. **SD WAN -** Software-Defined Wide Area Network - It's a technology that allows organisations to manage and optimise their wide area network (WAN) infrastructure using software-based controllers and application-level policies.

3. HOSTED FIREWALL SERVICES

3.1. The Fortinet Hosted Firewall service is provided by a virtualised or physical Fortigate Firewall device hosted on the Supplier's network that provides access control (firewalling) for a Customer that connects to the Supplier network via Layer 2 fibre services and/or Layer 2 wireless and/or L3 services or Fortinet SD-WAN.

3.2. The Service comprises 1 x VDOM (Virtual Domain) which equates to 1 Firewall instance.

3.3. The ruleset to be applied by the Supplier is dictated by the Customer. As the enforcer of the Customer's IT security policy, the Supplier takes no responsibility for rules which are requested via the official channels, even if those rules lead to undesired effects.

3.4. All changes to the ruleset must be communicated via email. Only changes from authorised technical contacts will be enacted.

3.5. The Customer may have read-only access to their VDOM, upon request.

3.6. Unified Threat Protection (UTP) services are an optional extra. The UTP services offered by the Supplier are:

3.6.1. Web Filtering

3.6.2. Application Control

3.6.3. Intrusion Prevention System (IPS)

3.6.4. User authentication (for Customers with Microsoft Active Directory)

3.6.5. Up to 3 IPSEC tunnels per VDOM

3.7. The Supplier will maintain N-2 firmware release on the Hosted firmwares provided. This is dependent on new bugs/features introduced in newer versions by the licensor.

3.7.1. This can be reviewed on a case-by-case basis. The Customer is responsible for requesting this change from the Supplier.

3.7.2. The Supplier has the right to approve or reject this request

3.7.3. The Supplier will patch all Hosted firewalls to a standard Firmware version. Should a serious vulnerability be detected by the Supplier or notified by the Licensor, these will be mitigated by applying the Licensor approved patch or security release

3.7.4. The Provider does not notify clients of Vendor software updates and Major and Minor releases.

3.8. The Supplier monitors the Vulnerability Reporting provided by FortiGate. These are remedied on an 'as needed' basis.

3.9. The Supplier will use all reasonable efforts to ensure that the customer's specified traffic blocking measures are implemented, however, given the intricate nature of network protocols and potential unforeseen circumstances, the Supplier cannot be held responsible for any unauthorized traffic that may circumvent these measures.

4. DEDICATED / ONSITE FIREWALL SERVICES

4.1. The Onsite Firewall service is an appliance provided by the Supplier to facilitate access control (firewalling) for a Customer's Internet access. The firewall is placed in-line and forms the gateway between the private network, DMZ's (Demilitrised Zone) and the public Internet.

4.2. The Service comprises of a physical Fortinet Firewall device/devices or Fortinet Firewall VM (Virtual Machines).

4.3. The ruleset to be applied by the Supplier is dictated by the Customer. As the enforcer of the Customer's IT security policy, the Supplier takes no responsibility for rules which are requested via the official channels, even if those rules lead to undesired effects.

4.4. All changes to the ruleset must be communicated via email to our Support Desk. Only changes from authorised technical contacts will be enacted.

4.5. The Customer may have read-only access to their FortiNet, upon request.

4.6. Unified Threat Protection (UTP) services are an optional extra if not purchased with the original firewall solution. The UTP services offered by the Supplier are:

4.6.1. Web Filtering as defined by the Fortinet Model specifications

4.6.2. Application Control as defined by the Fortinet's Model specifications

4.6.3. Intrusion Prevention System (IPS) as defined by the Fortinet Model specifications

4.6.4. User authentication (for Customers with Microsoft Active Directory)

4.6.5. IPSEC Tunnels as defined by the Fortinet Model specifications

4.7. The Supplier will maintain N-2 firmware release on the Hosted firmware's provided. This is dependent on new bugs/features introduced in newer versions.

4.7.1. This can be reviewed on a case-by-case basis. The Customer is responsible for requesting this change from the Supplier

4.7.2. The Supplier has the right to approve or reject this request

4.7.3. The Supplier maintains the same firmware version on all Dedicated Customer Firewalls. Should a serious vulnerability be detected by the Supplier or notified by the Licensor, these will be mitigated by applying the Licensor's approved patch or security release

4.7.4. The customer shall be solely responsible for the following

4.7.4.1. It's use of the Services under this Product Annexure and accesses same at its own risk

4.7.4.2. Any costs associated with Customer Premises Equipment (CPE) which, if requested by the Customer, may be provided by the Supplier pursuant to the terms of a separate CPE agreement, and/or

4.7.4.3. Local access and access-related changes, including any changes for interconnection, installation, inside wiring, construction, distance and termination charges and other access-related charges

4.7.4.4. During any term and thereafter any CPE provided by the Supplier for provision of the Service to be located at the Customer's premises will remain the property of the Supplier/licensor. The Equipment does not belong to the Customer, the Customer may not sell, lease, abandon, or give away the Equipment; allow anyone other than the Supplier/manufacturer to service the Equipment; or permit any other person to use the Equipment, other than on Customer's behalf in connection with Customer's use of the Fortinet Service. The Customer is directly responsible for the loss of the Equipment

4.7.4.5. The Customer agrees to abide by any terms of use for the Fortinet Service published by Fortinet. The Customer agrees not to disable or defeat any capacity-limiting feature of the Equipment, or otherwise use the Equipment at a greater capacity rate than the rate for which the Customer has subscribed. The Customer agrees not to use the Equipment with any unsupported hardware or software (as described in the applicable documentation provided by Fortinet); or use the Service other than as described in the documentation provided therewith or use the Fortinet Service for any unlawful purpose

4.7.4.6. The Customer shall, at its own expense, keep all CPE free and clear of any claims, liens, and encumbrances of any kind. Make no alterations or affix any additions or attachments to the CPE, except as approved by the Supplier in writing. Not remove, alter, or destroy any labels on the CPE and will allow the Supplier and Fortinet unrestricted access to the CPE for purposes of testing, upgrading and other maintenance activities. Take such action as is necessary to protect the CPE including but not limited to, the provision of a secure, rack mounted, air-conditioned space to house, and sufficient clean electricity to run the CPE, reasonable steps to protect the CPE against theft, abuse or misuse, and reasonable steps to protect the CPE against physical damage. Comply with all instructions and requirements of the Supplier or manufacturer's manuals regarding the care and use of the CPE. Assure that the CPE will be operated by competent and duly qualified personnel in compliance with all laws and regulations

4.7.4.7. The Customer further agrees to indemnify, defend, and hold harmless the Supplier and its respective officers, directors, employees, contractors, and agents against and from any loss, debt, liability, damage, obligation, claim, demand, judgement, or settlement including without limitation, attorneys' fees and all reasonable costs and expenses of litigation arising out of, or resulting from any CPE loss. In no event will CPE loss relieve the Customer of the obligation to pay The Supplier any amounts due under this Agreement

4.7.5. The Supplier does not notify Customers of licensor software updates and major and minor releases.

5. FIREWALL REPORTING - VFAZ

5.1. Firewall reporting is an optional extra, which can be provided by the Supplier's Virtual FortiAnalyzer (VFAZ) service.

5.1.1. Live logs are stored for 30 days, and archived logs are available for a further 30 days

5.1.2. Should longer retention be required, the Supplier can facilitate on a case-by-case basis

5.1.3. The amount of logs determines the monthly cost for log storage. Please refer to the Supplier price list for log volume costing

5.1.4. This will be a variable Fees based on the customer's monthly usage

5.2. For onsite firewalls, transmission of logs from the firewall to the VFAZ service inherently utilises some of the Customer's available WAN bandwidth.

6. REMOTE ACCESS SERVICES - FortiClient

6.1. Should Remote Access Services be required, secure VPN customer functionality would be supplied by the Supplier. This service allows remote users to securely connect to corporate resources, behind the firewall, over the public Internet. This functionality would be provided by the Forticustomer software.

6.1.1. For Hosted Firewall services, the service is based on a per-user billing model. Each additional user would require their own account configured on the FortiGate firewall. No sharing of user accounts is permitted.

6.1.2. For Dedicated/onsite firewall services, the Firewall's capability determines the number of user accounts that can be accommodated.

6.1.3. FortiClient must be downloaded and installed by the end user (or Customer IT administrator) and installed onto a supported version of Windows / MacOS / Linux / Apple IOS / Android.

6.1.4. The configuration profile will be supplied by the Supplier to the authorised Security Technical Contact/s. This will include the public IP address of the Firewall. It is the Customer's responsibility to create a DNS entry for this IP address if required.

6.1.5. Static (local) usernames and passwords will be configured on the Customer's FortiGate VDOM. Should LDAP integration into Microsoft Active Directory be required, this would incur an additional installation cost, which will be quoted case by case basis prior to project commencement.

6.1.6. End-user support would be performed by the Customer's IT administrator. The Supplier will support the administrator as part of the normal technical support process. Password resets should be logged by the authorised IT administrator, via email. New passwords may be sent directly to end-users via email.

6.2. SSL certificates are not included by default, and need to be sourced by the Customer

6.3. Should the Customer require a security management solution that enables scalable and centralised management of multiple endpoints (computers), the enterprise management server (EMS) can be provided by the Supplier. This solution is provided on a per-endpoint and per-user licensing model

6.4. EMS is used to deploy, configure, and monitor endpoints. In integrated mode, a FortiGate device is required, and NAC is supported. In integrated mode, EMS deploys FortiClient software on endpoints, and FortiClient endpoints connect FortiClient Telemetry to FortiGate to receive compliance rule

6.5. The EMS solution will entitle the Customer to the following functionality:

6.5.1. efficient and effective administration of endpoints running FortiClient

6.5.2. visibility across the network to securely share information and assign security profiles to endpoints

6.5.3. support for Fabric Agent for endpoint telemetry,

6.5.4. security posture check via ZTNA tagging,

6.5.5. remote access (SSL and IPsec VPN),

6.5.6. Vulnerability Scan,

6.5.7. Web Filter, and

6.5.8. threat protection via Sandbox (appliance only).

6.6. Once a device has been added to EMS via the Web Interface the Remote Management Tools can be used to perform configuration tasks on that device such as synchronising, calibrating and merging.

7. SERVICE FEES AND CHARGES

7.1. Service Fees shall be provided at the rates set out in the Supplier pricing plan at the time of subscription, plus applicable taxes. The Supplier may from time to time modify the Service Fees.

8. RESTRICTIONS

8.1. All orders are final, and the Products and Services are not returnable unless expressly permitted under the applicable Product warranty.

8.2. The Customer is prohibited from, and is responsible for preventing its employees and contractors from attempting to:

8.2.1. use the Software to determine, or disclose the results of, any benchmarking or performance measurements;

8.2.2. interfere with a platform for use of the Software;

8.2.3. use the Software on a device not owned and controlled by the Customer;

8.2.4. use automated means to access online portions of the platform for the Software;

8.2.5. use the Software for third-party training, commercial time-sharing, or service bureau use or (except as expressly set forth in this Agreement) use the Software to provide services to third parties,

8.2.6. share non-public features or content of the software with any third party;

8.2.7. access the software in order to build a competitive product or service, to build a product using similar ideas, features, functions, or graphics of the software, or to copy any ideas, features, functions, or graphics of the software; or,

8.2.8. engage in web scraping or data scraping on or related to the software, including without limitation, collection of information through any software that simulates human activity or any bot or web crawler.

8.3. The licensor and/or the Supplier may terminate the Customer's use of the Products and Services referred to in this Annexure, together with the licences and other rights herein, immediately without notice if the Customer breaches or fails to comply with any of the terms and conditions of this Annexure or the Contract Documents or for other reasons as stated in the licensor's other documentation. The Customer agrees that, upon such termination, it will cease using the Software and any Products and either destroy all copies of the documentation or return all materials to the Supplier or the licensor.

END OF ANNEXURE

On behalf of Saicom Voice Services (Pty) Ltd

Signed at _____ on the _____day of _____ 20__

_____

Signature

_____

Full Name

_____

Title

who warrants that they are duly authorised hereto

On behalf of {Client_Name}

Signed at _____ on the _____ day of _____ 20__

_____

t +27 (0) 10 140 5000 e sales@saicom.io w saicom.io

Signature

_____

Full Name

_____

Title

who warrants that they are duly authorised hereto